**Michael Chillemi**

**Hw10**

**Comp Net**

**29.17:**Many commercial firewall products allow a manager to specify packets to *deny* as well

as packets to *accept*. What is the disadvantage of a configuration that allows denial?

ANS:

The disadvantage is it is easier to write a rule of the packets that are allowed rather then specify a set of packets that are denied.

**29.18:**Rewrite the firewall configuration in Figure 29.9 to allow an outsider to *ping* each of the

three servers.

ANS:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Dir | Frame Type | IP Src | IP Dst | IP Type | Src Port | Dest port |
| In | 0x0800 | \* | 192.5.48.1 | TCP | \* | 80 |
| In | 0x0800 | \* | 192.5.48.2 | TCP | \* | 25 |
| In | 0x0800 | \* | 192.5.48.3 | TCP | \* | 53 |
| In | 0x0800 | \* | 192.5.48.3 | UDP | \* | 53 |
| In | 0x0800 | \* | 192.5.48.1 | ICMP |  |  |
| In | 0x0800 | \* | 192.5.48.2 | ICMP |  |  |
| In | 0x0800 | \* | 192.5.48.3 | ICMP |  |  |
| Out | 0x0800 | 192.5.48.1 | \* | TCP | 80 | \* |
| Out | 0x0800 | 192.5.48.2 | \* | TCP | 25 | \* |
| Out | 0x0800 | 192.5.48.3 | \* | TCP | 53 | \* |
| Out | 0x0800 | 192.5.48.3 | \* | TCP | 53 | \* |

**29.19:**Rewrite the firewall configuration in Figure 29.9 to move the email server to the computer running the web server.

ANS:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Dir | Frame Type | IP Src | IP Dst | IP Type | Src Port | Dest port |
| In | 0x0800 | \* | 192.5.48.1 | TCP | \* | 80 |
| In | 0x0800 | \* | 192.5.48.2 | TCP | \* | 25 |
| In | 0x0800 | \* | 192.5.48.3 | TCP | \* | 53 |
| In | 0x0800 | \* | 192.5.48.3 | UDP | \* | 53 |
| In | 0x0800 | \* | 192.5.48.1 | ICMP |  |  |
| In | 0x0800 | \* | 192.5.48.2 | ICMP |  |  |
| In | 0x0800 | \* | 192.5.48.3 | ICMP |  |  |
| Out | 0x0800 | 192.5.48.1 | \* | TCP | 80 | \* |
| Out | 0x0800 | 192.5.48.2 | \* | TCP | 25 | \* |
| Out | 0x0800 | 192.5.48.3 | \* | TCP | 53 | \* |
| Out | 0x0800 | 192.5.48.3 | \* | TCP | 53 | \* |

**29.20:**Read about commercial IDS systems, and make a list of attacks the systems can detect.

ANS:

* Port scanning
* SYN Flooding
* Open TCP connection
* Send UDP datagrams

29.22: Why isn’t deep packet inspection used on the highest-speed networks?

ANS:

They are not used on the highest speed networks they examine packet payloads which are much larger than packet headers and not organized into fixed fields, Deep Packet Inspection (DPI) mechanisms are limited to lower-speed networks.

**29.23**What are the two goals of a VPN system?

ANS:

* Extended connections across multiple geographic locations without using a leased line.
* Improved security for exchanging data.

**29.24**What are the three ways a VPN can transfer data across the Internet?

ANS:

* Payload encryption
* IP-in-IP tunneling
* IP-in-TCP tunneling

**29.25**When a VPN uses IP-in-IP tunneling, what prevents an attacker from reading the header

of the original datagram?

ANS:

It encrypts the entire datagram including the header.

**29.26**In some VPN systems, a sender appends a random number of extra zero bits to a datagram before encrypting, and the receiver uses the datagram length field to discards the extra bits after the datagram has been decrypted. Thus, the only effect of the random padding is to make the length of the encrypted datagram independent of the length of the unencrypted version. Why is the length important?

ANS:

Datagrams come in a variety of block sizes, which makes encrypting the data difficult. Because datagrams have a header and length field that aid in determining the data's original length, zeros are added to make the total length an exact multiple of block size. To make the plain text the exact multiple of the block size, a random length of padding is added. When a datagram packet is retrieved and encrypted, the extraneous zeroes are deleted, allowing the original content to be decoded. Extra padding zeroes are eliminated during decryption because they aren't required. This emphasizes the importance of length and the size of the correct multiple of block size.

**29.27**List eight security technologies used in the Internet, and describe the purpose of each.

ANS:

* *PGP* (*Pretty Good Privacy*). A cryptographic system that applications can use to encrypt data before transmission. PGP was developed at MIT, and is especially popular among computer scientists.
* *SSH* (*Secure Shell*). An application-layer protocol for remote login that guarantees confidentiality by encrypting data before transmission across the Internet.
* *SSL* (*Secure Socket Layer*). A technology originally designed by Netscape Communications that uses encryption to provide authentication and confidentiality. SSL software fits between an application and the socket API, and encrypts data before transmitting over the Internet. SSL is used on a web connection to allow users to conduct financial transactions safely (e.g., send a credit card number to a web server).
* *TLS* (*Transport Layer Security*). Designed by the IETF in the late 1990s as a successor to SSL, TLS builds on version 3 of SSL. Both SSL and TLS are available for use with HTTPS.
* *HTTPS* (*HTTP Security*). Not really a separate technology, HTTPS combines HTTP with either SSL or TLS and a certificate mechanism to provide users with authenticated, confidential communication over the Web. HTTPS uses TCP port 443 instead of port 80.
* *IPsec* (*IP security*). A security standard used with IP datagrams. IPsec uses cryptographic techniques, and allows the sender to choose authentication (i.e., validate the datagram’s sender and recipient) or confidentiality (i.e., encrypt the datagram payload).
* *RADIUS* (*Remote Authentication Dial-In User Service*). A protocol used to provide centralized authentication, authorization, and ac- counting. RADIUS is popular with ISPs that have dialup users and with VPN systems that provide access to remote users.
* *WEP* and *WPA* (*Wired Equivalent Privacy* and *Wi-Fi Protected Access*). WEP was originally part of the Wi-Fi wireless LAN standard, and was used to keep transmissions confidential. Researchers at U.C. Berkeley found several weaknesses in WEP, and WPA (later *WPA2*) was developed as a replacement.